

ENGLISH ABSTRACT OF DOCUMENT (1)
PATENT ABSTRACTS OF JAPAN

(11) Publication number : 2000-347808

(43) Date of publication of application : 15.12.2000

(51) Int.Cl. G06F 3/06

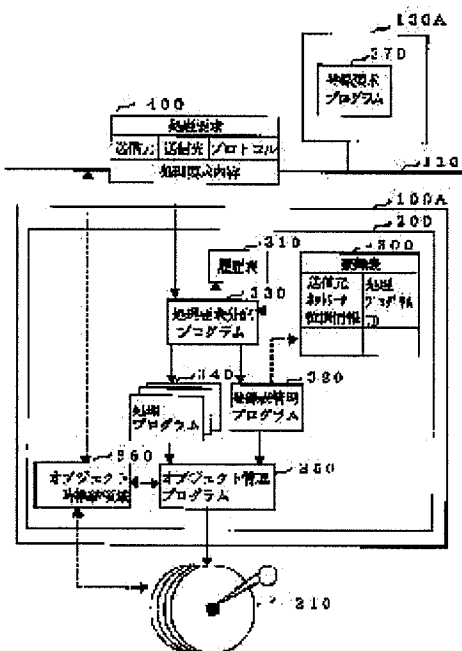
G06F 12/14

G06F 13/00

(21) Application number : 11-154646 (71) Applicant : HITACHI LTD

(22) Date of filing : 02.06.1999 (72) Inventor : TOMITA AKI
ODAWARA
HIROAKI

(54) DISK DEVICE DIRECTLY CONNECTABLE TO NETWORK



(57) Abstract:

PROBLEM TO BE SOLVED: To guarantee the security of a magnetic disk device directly connectable to a network by providing a means for discriminating whether a data processing request can be executed or not corresponding to the transmission source of a packet when the packet containing that data processing request is received. SOLUTION: A computer investigates whether or not a computer is registered on a registration table 300 and the protocol of requested processing is permitted or not. When it is registered and the protocol is permitted, a processing program 340 corresponding to the requested protocol is run. When it is not registered or the protocol is not registered, processing request

contents are recorded on a history table 310 and processing is finished. In this case, error contents are not returned to the processing request transmission source of a magnetic disk device 100A. Thus, the computer, which is not registered in the magnetic disk device 100A or whose protocol is not processed yet, can not know the existence of the magnetic disk device 100A.

LEGAL STATUS

CFO 16251 US

[Date of request for examination] 18.03.2003

[Date of sending the examiner's decision of rejection] 13.06.2006

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

【特許請求の範囲】

【請求項1】プログラムを実行可能なプロセッサと、データを記憶するための記憶媒体と、ネットワークへの接続機構と、上記ネットワークを介してデータ処理要求を含むパケットを受信した場合、そのパケットの送信元に応じてそのデータ処理要求が実行可能か否かを判定する手段とを有することを特徴とするネットワークに直接接続可能なディスク装置。

【請求項2】上記データ処理要求が要求する処理プロトコルに応じて、そのデータ処理要求が実行可能か否かを判定することを特徴とする請求項1に記載のネットワークに直接接続可能なディスク装置。

【請求項3】複数の処理プロトコルを処理する手段を有することを特徴とする請求項2に記載のネットワークに直接接続可能なディスク装置。

【請求項4】プログラムを実行可能なプロセッサと、データを記憶するための記憶媒体と、ネットワークへの接続機構と、上記ネットワークに接続された計算機のネットワークアドレスと、上記計算機が処理要求することができる処理プロトコルとを記憶手段に登録する手段と、上記ネットワークを介してデータ処理要求を受信した場合、そのデータ処理要求が上記登録された計算機であるか否かを判定する手段とを有することを特徴とするネットワークに直接接続可能なディスク装置。

【請求項5】上記データ処理要求が上記登録された処理プロトコルであるか否かを判定する手段を有することを特徴とする請求項4に記載のネットワークに直接接続可能なディスク装置。

【請求項6】上記記憶手段に登録するためのプロトコルを複数有することを特徴とする請求項4又は請求項5の何れかに記載のネットワークに直接接続可能なディスク装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワークに直接接続可能な磁気ディスク装置のアクセス制御方式に関する。

【0002】

【従来の技術】従来、磁気ディスク装置は、そのハードウェア制約のため、一定のブロックサイズに基づいてデータを管理し、Point-to-Point通信方式によりデータを転送する、といった簡単な機能しか提供していなかった。

【0003】ANSI (American National Standard Institute) が開発し、磁気ディスク装置と計算機間のインタフェースとして広く使用されている SCSI (Small Computer System Interface) にお

いては、ファイルやテーブルといった論理的に一塊のデータの単位ではなく、ブロック単位によりチャネル上でデータ入出力を行う。SCSIは低位なインタフェースしか提供しないので、ファイルやテーブルといった論理的な高位のインタフェースを実現するためには、磁気ディスク装置が直接接続される計算機上でファイルシステムやデータベース管理システムが実行されていた。

【0004】近年、ハードウェア技術の進歩と低価格化を背景として、ネットワークに接続するための機構を備え、磁気ディスク装置とデータ入出力を要求する計算機間に他の計算機を介さず直接データ入出力を行うことができる NASD (Network-Attached Secure Disk) がカーネギーメロン大学の G. Gibson により提案された (The 8th ASPLOS Conference 予稿集、1998 年)。NASD はネットワーク接続機構を備えているだけではなく、ファイルといった論理的に一塊のデータ単位に基づいてデータを管理する。

【0005】NASD では、磁気ディスク装置とデータ入出力を要求する計算機間に他の計算機を介さず直接データ入出力を行うことができるので、悪質な第三者が NASD に不正アクセスすることが可能である。そのため、NASD では、高いセキュリティを保証するために、暗号化技術を用いたプロトコルを提供している。

【0006】

【発明が解決しようとする課題】NASD への処理要求のセキュリティは、NASD プロトコルが実装されている通信階層において検証される。現在、NASD プロトコルは RPC (Remote Procedure Call) 上に実装されている。RPC は、一般には、OSI (Open Systems Interconnection) のトランスポート層に相当する UDP や TCP 上に実装される。つまり、NASD への処理要求のセキュリティはトランスポート階層よりも下位の、例えば、IP といったネットワーク層においては検証されない。たとえ、NASD のセキュリティ機構が処理要求は不法侵入か否かを検証するとしても、何度でも NASD のセキュリティ機構を破ろうと試みる事が可能であり、不法な処理要求は NASD プロトコルが実装されているネットワーク層以下の階層には到達している。

【0007】一般に、ネットワークに接続されている計算機には、例えば、NFS (Network File System) といった分散ファイルシステムや SNMP (Simple Network Management Protocol) といった管理サービスなどの複数のサービスプロトコルが登録されている。実際には、ネットワーク直接接続型ディスク装置も、NASD プロトコルだけといったように一つのサービスプロトコルだけではなく、複数のサービスプロトコルを提供可能であるように実装する可能性が高い。この場合、NASD プロトコル以外のサービスプロトコルのセキュリティ

が低いと、ディスク装置のセキュリティは保証されない。

【0008】そこで、本発明は、ネットワークに直接接続可能な磁気ディスク装置のセキュリティを保証することにある。

【0009】

【課題を解決するための手段】上記の課題を達成するために、本発明の磁気ディスク装置は、受け取った処理要求を該当するサービスプロトコルの処理部に処理要求を渡す前に、不法侵入か否かを判定するプログラムを実行する。磁気ディスク装置は処理要求の発行を許可している計算機のネットワーク上の位置情報を登録している。判定プログラムは登録されていないネットワーク上の位置を送信元とする処理要求であることを判定すると、不法侵入と見なして棄却し、その処理要求の記録をとる。

【0010】

【発明の実施の形態】本発明によるネットワークに直接接続された磁気ディスク装置のアクセス制御方式の一実施例を図面を用いて説明する。

【0011】[1] 構成の概略

図1は、本発明の磁気ディスク装置を用いたシステムのハードウェア構成例を示している。磁気ディスク装置100A、100B、100Cや計算機や磁気ディスク装置であるオブジェクト管理設定要求実体130A、130Bはネットワーク110で接続されている。磁気ディスク装置は、ファイルやテーブル、レコードといった論理的なデータ単位であるオブジェクト120A、120B、120Cを格納している。

【0012】図2は個々の磁気ディスク装置のハードウェア構成を示している。各磁気ディスク装置は、電源によりバックアップされているメモリ200、磁気ディスク媒体210、一つもしくは複数個のプロセッサ220を持つ。

【0013】図3は本発明の一実施例の構成を示している。磁気ディスク装置100Aは登録表300、履歴表310や登録表管理プログラム320、処理要求分配プログラム330、処理プログラム340、オブジェクト管理プログラム350をメモリ200に置いて実行する。登録表300は、磁気ディスク装置100Aを使用可能な計算機のネットワーク上の位置情報とその計算機に許可されている処理プロトコルの対を保持している。処理プロトコルの例としては、NASDプロトコルやSNMP (Simple Network Management Protocol)、JMAPI (Java Management API) が挙げられる。登録表管理プログラム320は、磁気ディスク装置100Aの電源を入れると磁気媒体210から読み出されて実行される。磁気ディスク装置100Aを管理する計算機130Aは磁気ディスク装置100Aを使用可能な計算機を登録するための登録要求プログラム370を保持す

る。

【0014】登録要求プログラム370を計算機130A上で手動でインストールして動作させることもできる。また、計算機130A上からWEBブラウザのようなネットワークアクセスプログラムを介して、磁気ディスク装置100Aから登録要求プログラム370を計算機130A上にダウンロードして動作させることもできる。さらに、登録要求プログラム370が動作する計算機130Aは登録表管理プログラム320が動作する磁気ディスク装置100Aと等しい場合もある。つまり、登録表管理プログラム320と登録要求プログラム370は同じ磁気ディスク装置100A上で動作させることもできる。磁気ディスク装置100Aの電源を入れて登録表管理プログラム320を磁気ディスク媒体210から読み出して実行すると、登録表管理プログラム320は、ディスプレイなどの表示装置に登録要求プログラム370を磁気ディスク装置100Aにおいて実行するか否か、という質問を表示する。磁気ディスク装置100Aにおいて実行するように指定された場合には登録要求プログラム370は磁気ディスク装置100A上で動作する。

【0015】磁気ディスク装置100Aは磁気ディスク装置100Aを使用可能な計算機を登録する際のプロトコルを複数保持することが可能である。磁気ディスク装置100Aを管理する計算機100Aは、登録に必要なセキュリティに応じて登録プロトコルを選択し、登録要求プロトコル370を介して選択したプロトコルに従って登録表管理プログラム320とやりとりして磁気ディスク装置100Aを使用可能な計算機を登録する。登録プロトコルの例としては、電子認証方式を用いたり、パスワードを用いたりするプロトコルが挙げられる。

【0016】オブジェクト管理プログラム350は処理プログラム340が発行する磁気ディスク媒体210上に格納されているオブジェクトの入出力要求を処理する。オブジェクト管理プログラム350は、磁気ディスク媒体210に書き込むオブジェクトや磁気ディスク媒体210から読み出したオブジェクトを一時的にオブジェクト一時格納領域360に格納する。

【0017】処理要求400は、計算機から磁気ディスク装置100Aに送信される処理要求の形式を示している。処理要求400は、送信元のネットワーク上の位置情報、送信先のネットワーク上の位置情報、プロトコルの種類等を保持する。ネットワーク上の位置情報の例としては、IPアドレスとポート番号の対が挙げられる。

【0018】本実施例では、磁気ディスク装置100Aを使用可能な計算機として計算機130Bが登録されている場合を想定する。図4は処理要求分配プログラム330の処理の流れを示している。まず、計算機130Bが登録表300に登録されており、要求する処理のプロトコルが許可されているか否かを調べる (ステップ50

0)。登録されており、かつ、プロトコルが許可されている場合には、要求するプロトコルに該当する処理プログラム340を実行する(ステップ510)。登録されていない、あるいは、プロトコルが許可されていない場合には、履歴表310に処理要求内容を記録して(ステップ520)終了する。この場合、磁気ディスク装置100A処理要求送信元にエラー内容を返さない。このことにより、磁気ディスク装置100Aに登録されていない、あるいは、プロトコルが処理されていない計算機は磁気ディスク装置100Aが存在したことも知ることができない。

【0019】

【発明の効果】本発明によれば、ネットワークに直接接

続可能な磁気ディスク装置へのアクセスを制限することにより、当該装置のセキュリティを保証することができる。

【図面の簡単な説明】

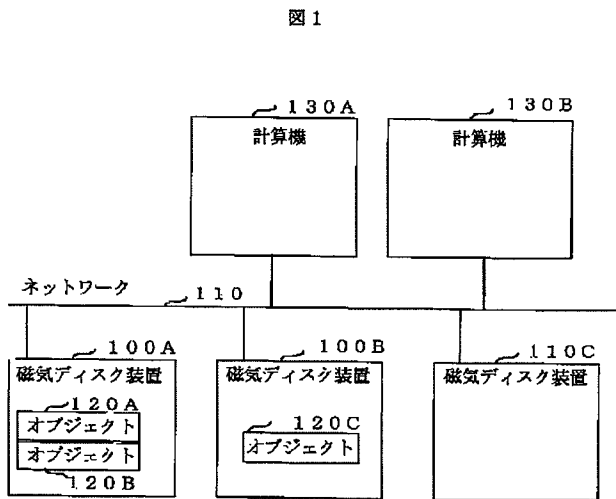
【図1】本発明の磁気ディスク装置の一実施例を示す図。

【図2】本発明の磁気ディスク装置のハードウェア構成を示す図。

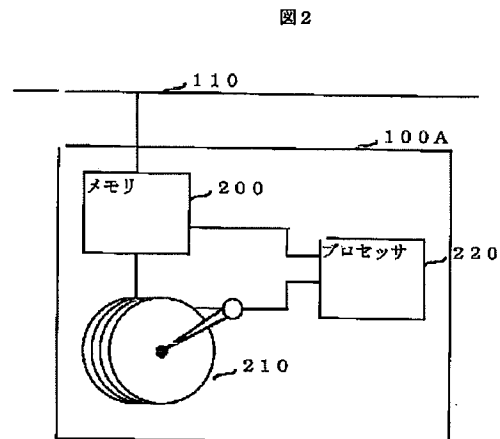
【図3】本発明の磁気ディスク装置に実装されるソフトウェア構成を示す図。

【図4】磁気ディスク装置の処理要求分配プログラムのフローチャートを示す図。

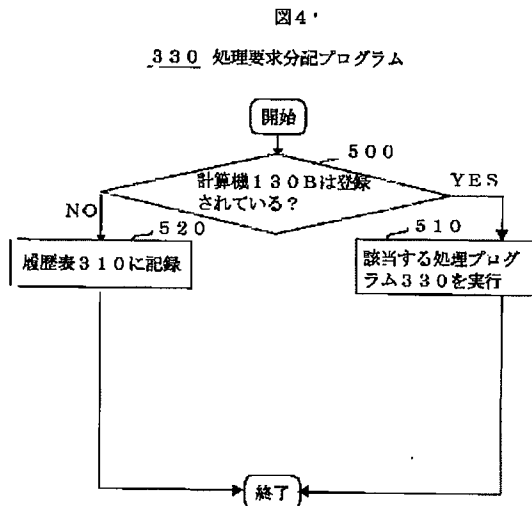
【図1】



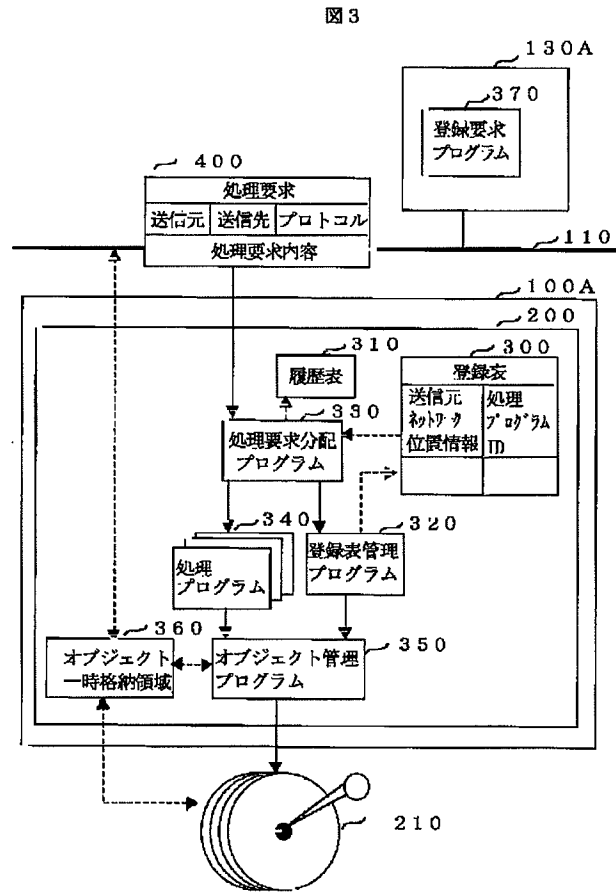
【図2】



【図4】



【図3】



フロントページの続き

Fターム(参考) 5B017 AA01 BA05 BA06 BA09 BB10
CA06 CA07 CA16
5B065 BA01 CA01 CE01 PA13 PA14
5B089 GA12 JA35 KA17 KB13